BROOKHAVEN NATIONAL LABORATORY

BNL Password Office

Strong Authentication Token Request Form

Return completed form in person (BNL badge MUST be presented as proof of ID) to:
ITD Password Office, Building 515, Rm. 1-34

NOTE: You will be contacted by the Password Office when your token is ready.

BNL applicants (w/ Life/Guest#) located primarily off-site may have a fellow on-site BNL employee turn in completed form, but Request Form must have been filled out & signed by off-site employee and must include copy of applicant's BNL badge. On-site employee must present badge when dropping off form. NON-BNL applicants will also need to have on-site BNL employee turn in the form (the approving supervisor who also signed this form) & show proof of ID.

Strong Authentication Token Requestor, please read, sign, and fill in the following information:

I have read the Statement on Proper Use of Strong Authentication Tokens and agree to abide by the policies listed therein.

Requestor's Signature:_____

Requestor's First Name: _____ Last Name: _____

BNL Dept:_____ Address/Bldg#: _____

BNL Phone#:_____ BNL Email Address:_____

*Life/Guest#: _____

***IF YOU DO NOT HAVE A LIFE/GUEST#, BE SURE TO FILL OUT ADDT'L INFO IN "NON-BNL USER" SECTION BELOW.**

If BNL employee located off-site, signature of on-site employee turning in Form:
Signature: _____ Print Name:_____ Life#:_____

********** NON-BNL USER **********

Non-BNL Users are required to provide the following additional information:

Company/Organization/Institution:_____

Department, if applicable:_____

Address:_____

Addt'l phone# where you can be reached:_____ Addt'l email address:_____

Anticipated timeframe for which you need access:_____

Reason for needing access to BNL network: _____

_____

Non-BNL Users MUST also have the signature of a BNL supervisor in the BNL department they are working with:

Approving Supervisor's Signature:_____ Date:_____

Approving Supervisor's First Name: _____ Last Name: _____

BNL Dept: _____ Address/Bldg#: _____

BNL Phone#: _____ BNL Email Address: _____

*Life/Guest#: _____

***Approving supervisors who have a Guest# MUST have signature authority in their particular department!**

For ITD Use Only

Token Serial Number:_____ Initial Expiration Date: / /
Type of Token: RB-1 (hard) _____ ST-1 (soft) _____ PT-1 (palm) _____ KF-1 (keyfob) _____ Other _____
Token Issuer Signature:_____
Date Token Issued:_____
User ID assigned:_____

For information re: CRYPTOCard tokens and their use, point your web browser to ITD's CyberSecurity web page.

CRYPTOCard Applicant's Name: _____

Dear Applicant,
In an effort to find the right kind of CRYPTOCard fit for each user, please answer as many of the following questions as you can. Return this questionnaire w/ completed Token Request Form to the Password Office. THANK YOU!!!

Do you currently use a SecureID token for access to lab machines? Yes _____ No _____

Are you using CryptoCard to access systems from off-site, on-site, or both?
(For example, AGS is testing implementing CryptoCard at their own internal Firewall, so workers may need to use the CryptoCard when here at the lab during work hours.)
Off-site only_____ On-site only _____ Both Off-site and On-site _____

If accessing the BNL network from **off-site only**, do you do so via the BNL IDAS system **ONLY**?
Yes _____ No _____

IMPORTANT!!!! **********
If you answered YES to **off-site access only** via **IDAS only**, **YOU DO NOT NEED A CRYPTOCARD TOKEN** at this time since you do not access the BNL network through the network perimeter firewalll… please discard your application if you have already turned it in!!!! THANK YOU!! Otherwise, please continue to answer the remaining questions below….
****

If accessing the BNL network from off-site, do you have the utility SSH on the machine(s) you will be working from?
Yes _____ No _____
If not, do you plan to load SSH on the machine(s)? **Yes_____ No _____**

If using SSH from an off-site machine, are you attempting to access UNIX machines, Windows-based machines (accessing files/email which will require you to be on the BNL network, such as users do with IDAS?), or both?
Unix machines only _____ Windows-based machines only _____ Both Unix & Windows _____

IMPORTANT!!!! **********
If you are using CryptoCard to access systems from **off-site only**, ***AND*** you are **using SSH only** from off-site (i.e., you have no plans to use telnet & ftp, except possibly thru IDAS), ***AND*** you are **accessing ONLY UNIX systems w/ SSH**, **YOU DO NOT NEED A CRYPTOCARD TOKEN** since SSH is allowed through the BNL network perimeter without additional authentication… please discard your application if you have already turned it in!!!! THANK YOU!! Otherwise, please continue to answer the remaining questions below….
****

Do you plan on working from one machine only when using the CryptoCard either from off-site or on-site, or will you be attempting access from several different machines?
Working from one machine only? **Yes _____ No _____**

List the type of system(s) (For example: UNIX, or PC w/ Windows) you will be working at when using the CryptoCard, and where are they located. (for example: UNIX system from offsite(home); PC loaded w/ Windows from onsite)

Machine Type (i.e., LINUX, UNIX, PC w/ Win): _____ Location (on-site, off-site): _____
Machine Type (i.e., LINUX, UNIX, PC w/ Win): _____ Location (on-site, off-site): _____
Machine Type (i.e., LINUX, UNIX, PC w/ Win): _____ Location (on-site, off-site): _____
Machine Type (i.e., LINUX, UNIX, PC w/ Win): _____ Location (on-site, off-site): _____

Do you already have knowledge of the various types of CryptoCards, and have an opinion on the type of CryptoCard you would like assigned to you? If so, please indicate what type of CryptoCard you require. (Refer to "Deciding on a CryptoCard Token" for guidance.)
Check one only: RB-1 hard token ____ KF-1 key fob ____ ST-1 soft token ____ PT-1 soft token ____ No preference ____

If accessing the network from off-site, do you plan on using only TELNET and FTP? **Yes _____ No _____**

If using something other than TELNET and FTP from off-site, please list what you believe you will be using… For example, do you plan on using an X-windowing application?

_____ _____ _____
_____ _____ _____

DECIDING ON A CRYPTOCARD TOKEN – Which Type Do I Want?

Currently, there are 4 types of CRYPTOCard Token to choose from. How do you decide which type you want?

The 4 types of CRYPTOCard Tokens:

RB-1 (*Hardware*-based Token which is metal-encased and about the size of a credit-card)
KF-1 (*Hardware*-based Token which is metal-encased and hangs on a key-chain)

ST-1 (*Software*-based Token application for Windows/Unix/Linux-based systems)
PT-1 (*Software*-based Token application for PalmPilots)

TOKEN	PROS	CONS
RB-1 (Hardware-based; credit-card sized)	- Easily portable for use from many machines.	- Can physically *forget* it and leave it behind; - Can be physically damaged by dropping, crushing, or sitting on it, by bending, twisting or carrying in hip pocket wallet, by immersing in water, by exposing it to extreme heat/cold, by dismantling it or by placing heavy objects on it.
KF-1 (Hardware-based; hangs on key-chain)	- Easily portable for use from many machines; - If attached to a key-chain, user less likely to *forget* it and leave it behind; - A bit less susceptible to physical damage than the RB-1 token since it can hang from a key-chain vs. attempting to carry in hip pocket wallet against vendor's recommendations.	- If user's token falls out of synch (which may happen occasionally) user CANNOT bring into synchronization themselves but instead must physically bring to Password Office to re-synch; - Currently, user cannot change their PIN on their own; - Although potentially less susceptible to physical damage than the RB-1, the KF-1 can *still* be damaged by dropping, crushing, or sitting on it, by bending or twisting, by immersing in water, by exposing it to extreme heat/cold, by dismantling it or by placing heavy objects on it.
ST-1 (Software-based for Windows, Unix, Linux)	- When application is loaded on a Windows, Solaris and/or Redhat Linux machine, user has no need to carry a physical token; - User can load software token application on more than one machine and more than one *type* of machine (i.e., can load on Windows machine AND on SUN Solaris machine AND on Redhat Linux machine); - When troubleshooting a token, Password Office can re-issue a new token without user needing to physically appear at Password Office.	- Argued to be slightly less secure than a hardware-version token since the 'something you have' aspect of strong authentication no longer has a true physical aspect to it (more on that at http://www.bnl.gov/cybersecurity/strong_auth.htm); - Software token application may not be available for certain computer platforms (i.e., VMS);
PT-1 (Software-based for PalmPilot)	- When Palm Pilot Token application loaded on user's Palm Pilot, no need for user to carry an additional physical device for authentication (i.e., an RB-1 or KF-1); - When troubleshooting a Palm token, Password Office can re-issue a new token without user needing to physically appear at Password Office.	- As with the ST-1 software token, Palm token is argued to be slightly less secure than a true hardware-version token; - If the user's PalmPilot crashes or otherwise causes Palm token program to disappear, Palm Pilot Token application has to be reinstalled.

BROOKHAVEN NATIONAL LABORATORY

BNL Password Office

Statement on Proper Use of Strong Authentication Tokens

You are being issued an Authentication Token for accessing Brookhaven National Laboratory Network and Computing Resources. This Token is for your use only, for work related functions. Issuance of this Token grants you no rights, but only validates that the person using this Token is actually you.

The Authentication Token, hereafter called Token, can take various forms, including a software program with an activation key, and a physical credit card like device. All forms of Tokens are treated equally, and carry the same conditions of use.

You agree not to divulge the PIN or accesses granted by the use of this card to anyone. Failure to abide by this will cause the immediate cancellation of the associated account, rendering the Token unusable. Further actions may be taken, up to and including dismissal for employees, or removal from the BNL property in the case of contractors, collaborators and all other non-BNL employees.

Actions arising from the misuse of this Token, and the resources available with its use are the responsibility of the person assigned to the Token. Since the use of this Token provides irrefutable authentication, unless reported stolen or compromised, it is the responsibility of the individual issued the Token to protect the Token against theft and misuse.

Use of this Token by any other party other then the person it is issued to will cause the Token to be deactivated, and disciplinary action taken, up to and including dismissal.

Loss or breakage of this Token will incur a charge of $75 to your BNL department or sponsoring organization for the replacement of the Token, and the resultant account maintenance.